AF SJFW

Practitioner's Docket No. 2337/107 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Martin A. Dorey

Application No.: 10/646,365 Group No.: 2181
Filed: 08/22/2003 Examiner: Kim, Harold J.
For: System, Device, and Method for Managing File Security Attributes in a Computer File Storage System

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on August 3, 2006.

2. STATUS OF APPLICANT

This application is on behalf of a small entity. A statement was already filed.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

*(When using Express Mail, the Express Mail label number is **mandatory**; Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

■ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
■ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
☐ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

☐ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

_____
Signature

Date: October 3, 2006

Jeffrey T. Klayman
(type or print name of person certifying)

** Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office to Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

small entity	$250.00
Appeal Brief fee due	**$250.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply. No extension is believed to be due.

The total fee due is:

Appeal brief fee	$250.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$250.00**

6. FEE PAYMENT

Attached is a check in the amount of $250.00.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 19-4972.

Date: October 3, 2006

Jeffrey T. Klayman
Registration No. 39,250
BROMBERG & SUNSTEIN LLP
125 Summer Street
Boston, MA 02110-1618
617-443-9292
Customer No. 02101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Martin A. Dorey	Docket No.:	2337/107
Appl. No:	10/646,365	Art Unit:	2181
File Date:	August 22, 2003	Examiner:	Kim, Harold J.

Invention: System, Device, and Method for Managing File Security Attributes In a Computer File Storage System

****

CERTIFICATE OF MAILING

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 3, 2006.

Jeffrey T. Klayman

****

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Table of Contents

10/06/2006 CNGUYEN 00000027 10646365
01 FC:2402 250.00 OP

Real Party in Interest

The real party in interest is BlueArc Corporation, the assignee of record.

Related Appeals and Interferences

Appellants' legal representative is not aware of any other appeals or interferences which will directly affect, or be directly affected by, or have a bearing on, the Board's decision in the present appeal.

Status of Claims

Claims 1-33 are pending in the application, and stand rejected under 35 U.S.C. 102(e) as being unpatentable over U.S. Patent No. 6,457,130 (Hitz).

The appeal, noticed August 3, 2006, is with respect to the rejected claims, claims 1-33.

Claim 29 is being withdrawn from consideration. Therefore, claims 1-28 and 30-33 remain under appeal.

Status of Amendments

As understood by Appellants, Appellants' amendments dated September 25, 2005 and June 20, 2006 were entered and considered by the Examiner.

Summary of Claimed Subject Matter

The present application relates to managing file security attributes in a computer file storage system supporting at least two file security models. A file is stored using a first file security model (e.g., UNIX). A client using a second file security model (e.g., Windows) accesses the file. A set of file security attributes in accordance with the second file security model is generated. The set of file security attributes includes a plurality of security identifiers (SID), including at least an owner SID and a group SID, that are derived from corresponding identifiers associated with the file in accordance with the first file security model. When the system is unable to map an identifier from the first file security model to an identifier for the second file security model, the generated SID includes both a map failure indicator and the corresponding identifier from the first set of file security attributes, such that the map failure indicator indicates that the identifier relates to the first file security model rather than to the second file security model. The map failure indicator therefore allows information about the map failure to be conveyed in the SID.

Independent claims 1, 16, and 31 clearly require a security identifier that includes separate map failure indicator and identifier components. Specifically, the claims expressly require "at least one map failure indicator" **AND** a "corresponding identifier." The description clearly shows that the SID includes separate map failure indicator and identifier components. In fact, all of the exemplary embodiments described in the specification clearly include a distinct map failure indicator in addition to the identifier (e.g., a distinct UNIX-specific authority identifier along with the UNIX identifier in exemplary UNIX-specific SIDs shown at page 8, line 19 and page 19, line 15, and a distinct UNIX-specific indicator along with a UNIX identifier as qualifiers to a well-known authority identifier value in an alternative embodiment described at page 19, lines 25-28). Thus, the claims unequivocally require two separate and distinct components, namely a map failure indicator and an identifier.

Independent claim 30 is directed to a method for generating, from a first set of file permissions in accordance with a first file security model, a second set of file permissions in accordance with a second file security model (see, for example, page 12, line 23

through page 15, line 19 and FIG. 4 of the application). The method involves translating the first set of file permissions into the second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions (see, for example, block 404 of FIG. 4 and page 12, line 23 through page 13, line 10); removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone (see, for example, block 406 of FIG. 4 and page 13, lines 16-18); adding any rights that need to be explicitly denied to the owner and to the group (see, for example, block 408 of FIG. 4 and page 13, line 18 through page 14, line 2); producing a set of access control elements ordered hierarchically (see, for example, block 410 of FIG. 4 and page 14, lines 4-18); and removing any redundant permissions from the access control elements (see, for example, block 414 of FIG. 4 and page 14, line 20 through page 15, line 6).

Independent claim 29 is being withdrawn from consideration.

Grounds of Rejection to be Reviewed on Appeal

Are claims 1-28 and 30-33 unpatentable under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,457,130 (Hitz), where Hitz clearly lacks a distinct map failure indicator?

Claim 29 is being withdrawn from consideration.

Argument Pages

Pertinent Chronology

The subject patent application was filed on August 22, 2003 with 33 claims.

An Information Disclosure Statement was filed on December 29, 2004 citing, among other things, the International Search Report and Written Opinion from the corresponding PCT application. Two pages from the International Search Report and Written Opinion are included in Appendix II. The relevance of these pages is discussed below.

A first office action issued on June 29, 2005 in which claims 1-33 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite due to the inclusion of trademarks in the claims and also under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,457,130 (Hitz).

A response to the first office action was filed on September 25, 2005 in which Applicants amended the claims to remove the trademark terms (even though MPEP 608.01(v) permits the use of trademarks that have a fixed and definite meaning, and even in view of the fact that Hitz's claims actually include trademark terms "Unix" and "NT"). Applicants also pointed out that Hitz does not disclose a map failure indicator in addition to the identifier, as required by the claims.

In the Final Office Action of April 3, 2006, Claims 1-33 were again rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,457,130 (Hitz).

A telephonic interview was held on May 10, 2006 between Supervisory Patent Examiner Fritz Fleming, Examiner Harold Kim, and Applicants' Attorneys Bruce Sunstein and Jeffrey Klayman regarding the final Office action dated April 3, 2006. Specifically, the Hitz reference was discussed in relation to the claimed invention. Applicants explained that Hitz describes a mixed Unix/Windows file storage system in which Unix file security attributes are mapped to Windows file security attributes when a Windows client accesses a Unix file. In Hitz, if a Unix name cannot be mapped to a corresponding Windows name, then the Unix name is returned to the Windows client

(Col. 6, lines 42-48), but Hitz does not include a specific map failure indicator to indicate that a mapping failure has occurred.

A response was filed on June 2, 2006 in which the Applicants explained that the claims of the subject patent application require **BOTH** a map failure indicator **AND** a corresponding identifier to be returned in the SID (specifically, "at least one map failure indicator **AND** the corresponding identifier from the first set of file security attributes," emphasis added). The map failure indicator and the identifier are clearly two distinct components. As expressed in the claims, the map failure indicator indicates that the identifier relates to the first security model (as opposed to the SID, which relates to the second security model).

Despite the plain wording of the claims and the described embodiments, which require both a distinct map failure indicator and a distinct identifier, the Examiner treats Hitz's simple identifier as both the map failure indicator and the identifier. Such an interpretation reads the word "and" out of the claim (with regard to requiring "at least one map failure indicator **AND** the corresponding identifier from the first set of file security attributes"), and also ignores the claim provision requiring that the map failure indicator indicate that the identifier relates to the first file security model. While Applicants conceded that the prior art shows one of the components – an identifier – there is utterly nothing in the prior art to satisfy the other leg of the claim – a map failure indicator.

An Advisory Action issued June 20, 2006 in which the Examiner essentially maintained his former position that the claims are anticipated by Hitz.

A Notice of Appeal, accompanied by a Pre-Appeal Brief, was filed on August 3, 2006.

A Panel Decision from Pre-Appeal Brief Review, mailed August 15, 2006, determined that there is at least one actual issue for appeal.

Thus, claims 1-33 remain pending and stand rejected.

Argument

It is well settled that a claim is invalid as anticipated under 35 U.S.C. § 102 only if a single prior art reference discloses either expressly or inherently, each limitation of the claim. *In re Cruciferous Sprout Litigation*, 301 F.3d 1343, 64 U.S.P.Q. 2d 1202 (Fed. Cir. 2002). Hitz simply does not disclose each and every limitation of the claim.

Independent claims 1, 16, and 31 clearly require a security identifier (SID) that includes separate map failure indicator and identifier components. Specifically, the claims expressly require "at least one map failure indicator **AND** the corresponding identifier from the first set of file security attributes" (emphasis added) or the like, and the description clearly shows that the SID includes separate map failure indicator and identifier components. In addition to ample support in the description for separate and distinct map failure indicator and identifier components (e.g., at page 8, line 19; page 19, line 15; and page 19, lines 25-28), Appellants note that the Examiner who prepared the International Search Report and Written Opinion for the corresponding PCT application (two pages of which are reproduced in Appendix II) clearly recognized that the map failure indicator and the corresponding identifier are two distinct components; in concluding that the claims meet novelty and inventive step requirements (with regard to the Allison reference), the Examiner stated that "the prior art does not disclose or suggest the specifically claimed SID including the UNIX-specific indicator and the corresponding UNIX identifier." Thus, it is clear that the claims unequivocally require two separate and distinct components, namely a map failure indicator and an identifier. U.S. Patent No. 6,457,130 (Hitz) generates a SID including only the identifier, and therefore fails to disclose separate and distinct map failure indicator and identifier components.

Furthermore, the claims expressly require that the map failure indicator indicate that the identifier relates to the first file security model, and this limitation is neither disclosed nor suggested by Hitz. As discussed in Hitz, UNIX user names and NT user names are merely alphanumeric strings (see, for example, Hitz column 6, lines 42-45), so there is nothing inherent in a user name to indicate the file security model to which it relates. In fact, the UNIX user names and NT user names are essentially fungible in that a UNIX user name can be used as an NT user name (see, for example, Hitz column 6, lines 45-48) and an NT user name can be used as a UNIX user name (see, for example,

Hitz column 7, lines 61-64). The Examiner argues that the Hitz's identifier acts as both the map failure indicator and the identifier. In fact, Hitz's identifier provides no indication of file security model in and of (and for) itself, and therefore Hitz's identifier cannot possibly act as the map failure indicator. Rather, as discussed and claimed in the subject patent application, a separate and distinct map failure indicator is used to indicate that the identifier relates to the first file security model. Hitz clearly lacks anything that can be considered a map failure indicator to indicate that the identifier relates to the first file security model.

It is clear, then, that Hitz fails to expressly or inherently disclose or suggest a map failure indicator as claimed. Hitz certainly does not disclose a map failure indicator that is separate and distinct from the identifier. Furthermore, Hitz's UNIX identifier simply cannot be both the map failure indicator and the identifier, as suggested by the Examiner, because the identifier does not indicate the file security model to which it relates. The fact that Hitz uses the UNIX user name as the NT user name is merely a result of a map failure; it does not indicate that a map failure has occurred (e.g., just because a person is sick does not mean that the doctor has been called). There is simply nothing in Hitz to indicate that a map failure has occurred.

For the reasons stated above, claims 1-28 and 31-33 are patentable over Hitz.

With regard to claims 15 and 30, the Examiner points to column 10, lines 1-17 of Hitz to show that Hitz translates a first set of file permissions into a second set of file permissions defining owner permissions, group permissions, and everybody permissions, as in claims 15 and 30. Such a translation, however, is merely one element of the methods defined in claims 15 and 30. These claims further require removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone; adding any rights that need to be explicitly denied to the owner and to the group; producing a set of access control elements ordered hierarchically; and removing any redundant permissions from the access control elements. The Examiner does not address these additional claim elements on any level. Furthermore, a close reading of Hitz, specifically column 10, lines 1-17, shows that Hitz does not teach or otherwise suggest such additional claim elements.

Thus, claim 30 is patentable over Hitz.

Conclusion

For the foregoing reasons, Applicant submits that claims 1-28 and 30-33 are allowable over the art of record and a decision of the Board to that effect is respectfully solicited.

Date: October 3, 2006

Respectfully submitted,

Jeffrey T. Klayman
Registration No. 39,250
Attorney for Applicant

Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110-1618
Ph.: (617) 443-9292
Fax: (617) 443-0004

02337/00107 547935.1

Appendix I: Claims Appendix

Claim 1 (previously presented): A method for managing file security attributes by a file server in a computer file storage system, the computer file storage system including a file secured using a first file security model, the method comprising:

receiving a first request from a client relating to the file stored in the computer file storage system, the client utilizing a second file security model;

retrieving a first set of file security attributes, in accordance with the first file security model, associated with the file, the first set of file security attributes including at least an owner identifier and a group identifier; and

generating a second set of file security attributes, in accordance with the second file security model, from the first set of file security attributes, the second set of file security attributes including a plurality of security identifiers (SID) including at least an owner SID derived from the owner identifier and a group SID derived from the group identifier, wherein at least one of the owner SID and the group SID includes at least one map failure indicator and the corresponding identifier from the first set of file security attributes, wherein the map failure indicator indicates that said identifier relates to the first file security model.

Claim 2 (previously presented): A method according to claim 1, wherein the at least one map failure indicator includes an authority identifier, specific to the first file security model, and an owner/group indicator having a first value to indicate that the identifier is

the owner identifier from the first set of security attributes, and a second value to indicate that the identifier is the group identifier from the first set of security attributes.

Claim 3 (previously presented): A method according to claim 1, wherein the at least one map failure indicator includes an authority identifier, specific to the first file security model, having a first value to indicate that the identifier is the owner identifier from the first set of file security attributes and a second value to indicate that the identifier is the group identifier from the first set of file security attributes.

Claim 4 (previously presented): A method according to claim 1, wherein generating the second set of file security attributes from the first set of file security attributes comprises:

attempting to map each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes; and

generating, for each identifier from the first set of file security attributes that cannot be mapped to a corresponding identifier from the second set of file security attributes, the SID including the at least one map failure indicator and the corresponding identifier from the first set of file security attributes.

Claim 5 (previously presented): A method according to claim 4, wherein attempting to map each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes comprises:

maintaining a table mapping a first set of names in accordance with the first file security model to a second set of names in accordance with the second file security model;

determining a name from the first set of names corresponding to the identifier from the first set of file security attributes; and

searching the table for a name from the second set of names corresponding to the name from the first set of names.

Claim 6 (previously presented): A method according to claim 5, wherein determining a name from the first set of names corresponding to the identifier from the first set of file security attributes comprises:

maintaining a cache mapping identifiers from the first set of file security attributes to names in the first set of names; and

searching the cache for a name from the first set of names corresponding to the identifier from the first set of file security attributes.

Claim 7 (previously presented): A method according to claim 5, wherein determining a name from the first set of names corresponding to the identifier from the first set of file security attributes comprises:

sending the identifier from the first set of file security attributes over a communication link to a NIS server; and

receiving the name from the first set of names over the communication link from the NIS server.

Claim 8 (previously presented): A method according to claim 1, further comprising:

transmitting the second set of file security attributes to the client in a response to the first request.

Claim 9 (previously presented): A method according to claim 8, further comprising:

receiving a second request from the client utilizing the second file security model including at least one of said SIDs including at least one map failure indicator and the corresponding identifier from the first set of file security attributes;

translating the at least one of said SIDs into a text string; and

transmitting the text string to the client in a response to the second request.

Claim 10 (previously presented): A method according to claim 9, wherein the text string includes a representation of the identifier from the SID.

Claim 11 (previously presented): A method according to claim 1, wherein the first set of file security attributes includes a first set of file permissions, in accordance with the first file security model, and wherein generating the second set of file security attributes from the first set of file security attributes further comprises:

generating a second set of file permissions, in accordance with the second file security model, from the first set of file permissions.

Claim 12 (previously presented): A method according to claim 11, wherein the request comprises at least one requested change to the security attributes of the file, and wherein the method further comprises:

applying the requested security attribute changes to the second set of file security attributes to create a modified set of file security attributes in accordance with the second file security model; and

writing the modified set of file security attributes to the file, said writing effectively changing the security model of the file from the first file security model to the second file security model.

Claim 13 (previously presented): A method according to claim 12, further comprising:

receiving a second request from a client utilizing the first file security model relating to the file, the second request associated with a session, the session having a session owner and a session group;

retrieving the modified set of file security attributes for the file; and

providing the client with owner access to the file, if the owner SID in the modified set of file security attributes includes an owner identifier in accordance with the first file security model and the session owner matches the owner identifier in the owner SID.

Claim 14 (previously presented): A method according to claim 12, further comprising:

receiving a second request from a client utilizing the first file security model relating to the file, the second request associated with a session, the session having a session owner and a session group;

retrieving the modified set of file security attributes for the file; and

providing the client with group access to the file, if the group SID in the modified set of file security attributes includes a group identifier in accordance with the first file security model and the session group matches the group identifier in the group SID.

Claim 15 (previously presented): A method according to claim 11, wherein generating the second set of file permissions from the first set of file permissions comprises:

translating the first set of file permissions into a second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions;

removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone;

adding any rights that need to be explicitly denied to the owner and to the group;

producing a set of access control elements ordered hierarchically; and

removing any redundant permissions from the access control elements.

Claim 16 (previously presented): An apparatus for managing file security attributes in a computer file storage system, the computer file storage system including a file secured

using a first file security model, the file associated with a first set of file security attributes including an owner identifier and a group identifier, the apparatus comprising:

a network interface for communicating with clients over a communication network;

a storage interface for communicating with a file storage device; and

file security logic operating between the network interface and the storage interface for managing file security attributes, the file security logic including logic for generating a second set of file security attributes, in accordance with a second file security model, from the first set of file security attributes, the second set of file security attributes including at least an owner SID derived from the owner identifier and a group SID derived from the group identifier, wherein at least one of the owner SID and the group SID includes at least one map failure indicator and the corresponding identifier from the first set of file security attributes, wherein the map failure indicator indicates that said identifier relates to the first file security model.

Claim 17 (previously presented): An apparatus according to claim 16, wherein the at least one map failure indicator includes an authority identifier, specific to the first security model, and an owner/group indicator having a first value to indicate that the identifier is the owner identifier from the first set of file security attributes and a second value to indicate that the identifier is the group identifier from the first set of file security attributes.

Claim 18 (previously presented): An apparatus according to claim 16, wherein the at least one map failure indicator includes an authority identifier, specific to the first file security model, having a first value to indicate that the identifier is the owner identifier from the first set of file security attributes and a second value to indicate that the identifier is the group identifier from the first set of file security attributes.

Claim 19 (previously presented): An apparatus according to claim 16, wherein the file security logic comprises:

logic for mapping each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes; and

logic for generating, for each identifier from the first set of file security attributes that cannot be mapped to a corresponding identifier from the second set of file security attributes, the SID including the at least one map failure indicator and the corresponding identifier from the first set of file security attributes.

Claim 20 (previously presented): An apparatus according to claim 19, further comprising a table mapping a first set of names, in accordance with the first file security model, to a second set of names, in accordance with the second file security model, the file security logic determining a name from the first set of names corresponding to the identifier from the first set of file security attributes and searching the table for a name from the second set of names corresponding to the name from the first set of names for mapping each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes.

Claim 21 (previously presented): An apparatus according to claim 20, further comprising a cache mapping identifiers from the first set of file security attributes to names in the first set of names, the file security logic searching the cache for a name from the first set of names corresponding to the identifier from the first set of file security attributes for determining a name from the first set of names corresponding to the identifier from the first set of file security attributes.

Claim 22 (previously presented): An apparatus according to claim 20, wherein the file security logic sends the identifier from the first set of file security attributes over a communication link to a NIS server for determining a name from the first set of names corresponding to the identifier from the first set of file security attributes.

Claim 23 (original): An apparatus according to claim 16, wherein the file security logic further comprises:

logic for translating the at least one of said SIDs into a text string.

Claim 24 (previously presented): An apparatus according to claim 23, wherein the text string includes a representation of the identifier from the SID.

Claim 25 (previously presented): A method according to claim 16, wherein the first set of file security attributes includes a first set of file permissions, in accordance with the first file security model, and wherein the file security logic further comprises:

logic for generating a second set of file permissions, in accordance with the second file security model, from the first set of file permissions.

Claim 26 (previously presented): An apparatus according to claim 25, wherein the file security logic includes logic for receiving a request from a client utilizing the second file security model, to modify file security attributes, applying the requested modifications to the second set of file permissions to create a modified set of file security attributes in accordance with the second file security model, and writing the modified set of file permissions to the storage device so as to effectively change the security model of the file from the first file security model to the second file security model.

Claim 27 (previously presented): An apparatus according to claim 25, wherein the file security logic includes logic for controlling access to the file using the second set of file permissions.

Claim 28 (previously presented): An apparatus according to claim 25, wherein the file security logic includes logic for translating the first set of file permissions into ~~a~~ the second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions; removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone; adding any rights that need to be explicitly denied to the owner and to the group; producing a set of access control elements ordered hierarchically; and removing any redundant permissions from the access control elements.

Claim 29 (currently withdrawn from consideration): An apparatus for managing file security attributes in a computer file storage system, the apparatus comprising:

means for translating an owner identifier in accordance with a first file security model into an owner SID, compatible with a second file security model;

means for translating a group identifier in accordance with a first file security model into a group SID, compatible with the second file security model; and

means for translating file access permissions, in accordance with a first file security model, into an access control list, compatible with the second file security model.

Claim 30 (previously presented): A method for generating, from a first set of file permissions in accordance with a first file security model, a second set of file permissions in accordance with a second file security model, the method comprising:

translating the first set of file permissions into the second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions;

removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone;

adding any rights that need to be explicitly denied to the owner and to the group;

producing a set of access control elements ordered hierarchically; and

removing any redundant permissions from the access control elements.

Claim 31 (previously presented): A method comprising:

receiving a security identifier (SID) including at least one map failure indicator and a corresponding identifier in accordance with a first file security model; and

translating the SID into a text string.

Claim 32 (previously presented): A method according to claim 31, wherein the text string includes a representation of the identifier from the SID.

Claim 33 (previously presented): A method according to claim 31, wherein translating the SID into a text string comprises:

transmitting a request to a translator over a communication network, the request including at least the identifier from the SID.

Appendix II: Evidence Appendix

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (SEPARATE SHEET)

International application No. PCT/US2004/017945

Group 2, Claim 30:

Group 2 solves the objectively determined problem of how to generate a Windows ACL from UNIX file permissions. This problem is solved by the method steps of claim 30.

These groups of inventions address entirely different technical problems and as such can be implemented independently of each other.

Hence, the application relates to a plurality of inventions, or groups of inventions, in the sense of Rule 13.1 PCT.

In the opinion of this International Examining Authority group 1 appears to relate to the main invention.

Re Item V
Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: BRIDGET ALLISON ET ALL: "File System Security: Secure Network Data Sharing for NT and UNIX" USENIX, [Online] 5 August 1998 (1998-08-05), pages 1-13, XP002306906 USA Retrieved from the Internet: URL:https://www.usenix.org/publications/library/proceedings/lisa-nt98/full_papers/allison/allison.pdf> [retrieved on 2004-11-22]
D2: US-B-6 446 1291 (DEFOREST MILES A ET AL) 3 September 2002 (2002-09-03)
D3: US 2002/112045 A1 (TYAGI VIKAS ET AL) 15 August 2002 (2002-08-15)

1. Independent claims 1, 16 and 31.

Document D1, which is considered to represent the most relevant state of the art, discloses (see par. 1 to 3 and par. 8 to 10) a method for managing file security attributes by a file server from which the subject-matter of claim 1 differs in that the

owner (group) SID includes an UNIX-specific indicator and the corresponding UNIX identifier.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

The problem to be solved by the present invention may be regarded as how to ensure that a Windows client accessing a UNIX-secured file of a file server receive from said file server a proper security descriptor for said accessed file.

The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) since the prior art does not disclose or suggest the specifically claimed SID including the UNIX-specific indicator and the corresponding UNIX identifier.

The apparatus described in claim 16 corresponds to the method disclosed in claim 1. As a consequence the above statements apply also for claim 16.

The method of claim 31 is also new and inventive since the subject-matter describes inter alia the SID including the UNIX-specific indicator and the corresponding UNIX identifier, feature that is not disclosed or suggested in the prior art.

2. Dependent claims 2-15, 17-28, 32 and 33.

Claims 2-15, 17-28, 32 and 33 are dependent on claims 1, 16 and respectively 31 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

3. Independent claim 30.

Document D1, which is considered to represent the most relevant state of the art, discloses (see par. 1 to 3 and par. 8 to 10) a method for generating a set of Windows file permissions from a set of UNIX file permissions from which the subject-matter of claim 30 differs in the steps of removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone; adding any rights that need to be explicitly denied to the owner and to the group; producing a set of

Appendix III: Related Proceedings Appendix

None.